"Express Mail" Label No. EV780616570US
Date of Deposit: March 27, 2006

PATENT
Attorney Docket No.: 040048-000110US

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Address" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By: Nina L. McNeill
Nina L. McNeill

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:

Paul Turgeon

Application No.: ~~10/086,796~~ 10086793

Filed: March 1, 2002

For: SYSTEM AND METHOD FOR PERFORMING SECURE REMOTE REAL-TIME FINANCIAL TRANSACTIONS OVER A PUBLIC COMMUNICATIONS INFRASTRUCTURE WITH STRONG AUTHENTICATION

Confirmation No. 1539

Examiner: Badii, Behrang

Art Unit: 3621

APPEAL BRIEF UNDER 37 CFR §41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellant offers this Brief in support of the Notice of Appeal submitted concurrently.

1. Real Parties in Interest

The real parties in interest are NYCE Corporation and Metavante Corporation.

2. Related Appeals and Interferences

This application is a continuation-in-part of U.S. Pat. Appl. No. 09/394,143, which was considered by the Board as part of prior Appeal No. 2005-2484. That prior appeal may be related to or otherwise have a bearing on the Board's decision in the current appeal.

A copy of the Board's decision in the prior appeal is attached in the Related Proceedings Appendix below.

3. Status of Claims

Claims 1 – 15, 40 – 54, 61 – 69, and 77 – 90 are pending in the application. All of these claims stand rejected pursuant to a Final Office Action mailed December 27, 2005 ("the Final Office Action").

The rejections of each of Claims 1 – 15, 40 – 54, 61 – 69, and 77 – 90 are believed to be improper and are the subject of this appeal.

4. Status of Amendments

No amendments have been filed subsequent to the mailing of the Final Office Action on December 27, 2005.

5. Summary of Claimed Subject Matter

The claimed invention relates to performing secure financial transactions over a public-access network (Application, p. 1, ll. 13 – 14). The Application illustrates applications in which the public-access network is the Internet, noting the need to protect transaction information when parties are involved in electronic commerce over such a network (*see, e.g., id.*,

p. 2, ll. 4 – 21). A particular difficulty in enabling such secure electronic commerce has been in transactions where funds are drawn directly from customer deposit accounts in the form of "debit" transactions (*id.*, p. 4, ll. 17 – 23).

Embodiments of the invention make use of a pair of ATM-network-compatible personal identification numbers ("PINs") in combination with other information to enable such transactions (*id.*, p. 5, ll. 8 – 15). The arrangement permits a standard CD-ROM drive in a personal computer to accept an instrument that may be used similarly to an ATM card, but over a public network like the Internet instead of over a secure private network like an ATM network (*id.*, p. 4, ll. 19 – 23). For instance, a portable storage medium readable by the CD-ROM and having certain information stored on it may be used as an e-commerce debit card (*id.*, p. 8, ll. 12 – 17). In illustrations described in the application, one of the PINs is a valid PIN and another of the PINs is an invalid PIN (*id.*, p. 25, ll. 21 – 22). Multiple layers of encryption are used to protect this information in addition to other information. To focus on those aspects of relevance to the pending claims, the summary description of those layers of encryption are simplified in this Brief; a detailed description of the encryption is provided in the specification of the Application.

A schematic of the encryption is illustrated with Fig. 4 of the Application. In addition to the two ATM-network-compatible PINs, the arrangement may additionally use an e-PIN, which is distinct from either of the ATM-network-compatible PINs and is used as an identifier over the public network (*id.*, p. 9, ll. 11 – 17). The valid and invalid ATM-network compatible PINs are each encrypted under a first key ("Key A") (*id.*, p. 26, ll. 7 – 12). Information derived using the e-PIN is encrypted under a separate key ("Key C") (*id.*, p. 26, ll. 12 – 15). Each of these encrypted pieces of information is combined with other customer data into a single data element that is encrypted under yet another key ("Key D") (*id.*, p. 26, ll. 18 – 22) to produce a binary large object ("BLOB") (*id.*, p. 27, ll. 1 – 4; *see also id.*, p. 13, ll. 5 – 8).

When a customer wishes to execute a transaction over the public network, the BLOB is supplied from the portable storage medium and a purported e-PIN is supplied by the customer (*id.*, p. 43, ll. 1 – 14; p. 46, ll. 12 – 16). This information is thus provided as a payment service request. A series of decryptions are performed on the payment service request to permit

comparison of the purported e-PIN with the e-PIN information recorded in encrypted fashion in the BLOB (*id.*, p. 61, ll. 9 – 19), thereby verifying the authenticity of the request. Irrespective of whether this verification is successful, a network transaction message is generated for transmission over the ATM network (*id.*, p. 62, ll. 7 – 11). If the e-PIN is valid, this network transaction message includes the encrypted valid ATM-network-compatible PIN (*id.*, p. 61, ll. 21 – 23), but if the e-PIN is invalid, this network transaction message includes the invalid encrypted ATM-network-compatible PIN (*id.*, p. 61, l. 23 – p. 62, l. 2). This permits the transaction to be processed as an ATM-network transaction based on the PIN information included in the network transaction message without the possibility of the valid ATM-network compatible PIN ever being available over the public network in unencrypted form — it is not accessible by a merchant party nor even accessible from information entered by the customer, who only enters the e-PIN (*id.*, p. 10, ll. 2 – 7). The transaction is processed accordingly and receipt of invalid PIN requests by issuers permits tracking of invalid PIN attempts as part of a fraud-detection technique (*id.*, p. 62, ll. 13 – 20).

a. Independent Claim 1

Each of the pending independent claims embraces aspects of having a payment service request that includes a pair of network-compatible PINs, with one of them being included in an ATM network transaction message depending on a result of validating independent identification information. Thus, Claim 1 recites a method of providing a payment service. A payment service request that has independent identification information and a pair of ATM-network-compatible PINs is received. With respect to the illustrative embodiment described above, this may be in the form of a purported e-PIN provided by a customer and a BLOB retrieved from a portable storage medium (*id.*, p. 43, ll. 1 – 14; p. 46, ll. 12 – 16). The independent identification information is validated, such as by validating the purported e-PIN as described in connection with the illustrative embodiment above (*id.*, p. 61, ll. 9 – 19). An ATM network transaction message containing at least one of the pair of ATM-network-compatible

PINs is generated based on such validation and forwarded to a financial institution over an ATM network for payment (*id.*, p. 62, l. 7 – p. 62, l. 20).

b. Independent Claim 40

Independent Claim 40 recites a system for providing a payment service. It recites a processor for processing a payment service request that has the independent identification information and the pair of ATM-network-compatible PINs described above (*id.*, p. 43, ll. 1 – 14; p. 46, ll. 12 – 16; the processor may be an Internet Intercept Processor, identified in the specification as an "IIP," *id.*, p. 13, l. 16). The processor is configured to perform those functions recited in independent method Claim 1.

c. Independent Claim 61

Like independent Claim 1, independent Claim 61 recites a method of providing a payment service. But the limitations recited in this claim are generally more detailed than those recited in independent Claim 1. An encoded data storage device is provided to a user (*id.*, p. 40, ll. 12 – 23). The data storage device has data representing a first ATM-network compatible PIN that is a valid ATM PIN associated with the user's account at a financial institution (*id.*, p. 26, ll. 7 – 9). It also has data representing a second ATM-network compatible PIN that is an invalid ATM PIN not associated with the user's account (*id.*, p. 26, ll. 9 – 12). Independent identification information is provided (such as in the form of an e-PIN) and validated (*id.*, p. 61, ll. 9 – 19). A payment service request is generated and includes a selected one of the first and second ATM PINs, depending on the validation, to be forwarded to the user's financial institution over an ATM network for further processing (*id.*, p. 62, l. 7 – p. 62, l, 20).

d. Independent Claim 77

Independent Claim 77 is a system claim that recites limitations using means-plus-function language. A first means is provided for generating a payment service request having independent identification information and a pair of ATM-network-compatible PINs (*e.g.*, *id.*, p. 43, ll. 1 – 14; p. 46, ll. 12 – 16). A second means is provided for validating the independent identification information (*e.g.*, *id.*, p. 61, ll. 9 – 19). A third means is provided for generating an ATM network transaction message containing at least a selected one of the ATM-network-compatible PINs based as least in part of the validation (*e.g.*, *id.*, p. 62, l. 4 – 20). A fourth means is provided for generating an ATM network transaction message to a financial institution over an ATM network for payment (*id.*, p. 62, l. 4 – 20). Examples of structure described in the specification for performing these various functions include the Internet Intercept Processor, an Active Web Component, a Merchant Payment Module, and a Hardware Security Module (*see id.*, Fig. 1; p. 13, l. 13 – p. 15, l. 22).

6. Grounds of Rejection to be Reviewed on Appeal

Whether Claims 1 – 15, 40 – 54, 61 – 69, and 77 – 90 are unpatentable over U.S. Pat. Publ. No. 2004/0199467 ("Martin") in view of U.S. Pat. No. Re38,255 ("Levine") and IBM Research Disclosure RD414097 ("IBM"). The Examiner's position on this issue is described on pp. 3 – 9 of the Final Office Action, supplemented by certain remarks on p. 2 of the Final Office Action captioned "Response to Arguments."

7. Argument

For a rejection to be maintained under 35 U.S.C. §103(a), the Examiner is charged with factually supporting a *prima facie* case of obviousness. Manual of Patent Examining Procedure, Eighth Edition, Third Revision, August 2005, 2131. Such a *prima facie* case requires, *inter alia*, that all limitations of the claims be taught or suggested by the cited references. In this instance, none of the cited references teaches suggests those limitations

recited in the independent claims directed at a payment service request having a pair of ATM-network-compatible PINs.

Before discussing each of the independent claims in turn, it is useful to consider the context of the cited art, particularly with respect to the use of PINs.

a. Cited Prior Art

Martin is relied on in the Final Office Action for most of the limitations of the claims, although the Final Office Action generally acknowledges that it fails to disclose a payment service request having a pair of ATM-network-compatible PINs (*see, e.g.*, Final Office Action, p. 3, l. 22). Instead, the Final Office Action relies on Levine and IBM for such a disclosure (*id.*, p. 3, ll. 22 – 23).

i. Levine

Appellant disagrees that Levine discloses a payment service request having a pair of ATM-network-compatible PINs. The Final Office Action cites three passages in Levine in support of its characterization, one of which is:

> The account database is consulted, looking up the entries corresponding to that BIN (step J). Once that sector of the database is located, the particular account number is located (step K). The inventory status data stored with the account number is located (step K). The inventory status data stored with the account number is checked to determine if the serial number received was distributed to that sales agent. The customer data and currency amount is then entered into the blank fields corresponding to that account number in the database (step L). The account number and the PIN number stored in the database (or a new PIN number transmitted by the customer) are then transmitted to the VisaNet system for updating of the PCAS software (step M). Finally, an acknowledgement message is sent back to the sales agent (step N).
> (Levine, Col. 6, ll. 11 – 24).

This passage is cited in the Final Office Action at p. 5, l. 6 and at p. 8, ll. 3 – 4, and describes generally the operation of software at an agent terminal. The passage suggests that the PIN that is transmitted is normally a PIN stored in a database, but could be "a new PIN transmitted by a

customer." Nothing in the passage suggests the simultaneous inclusion of both these PINs as part of a payment service request. As described in the passage, only a single PIN is ever actually transmitted "to the VisaNet system," with the disclosure merely noting that that single PIN might be drawn from a database or might be transmitted by a customer.

The Final Office Action also cites:

> [The] ATM also transmits a currency code which show what currency is in the ATM. The VisaNet network performs any required currency translation (step D). The ETC processor software then looks up the card number in the database (step E), and the PIN number associated with the account in the database is compared to the transmitted PIN number (step F). If the PINs don't match, a return error message is transmitted to the ATM (step G).
> (Levine, Col. 7, ll. 1 – 9).

This passage is cited numerous times in the Final Office Action at p. 3, l. 24; at p. 4, l. 21; at p. 5, l. 3; at p. 5, l. 6; at p. 6, l. 4; and p. 8, l. 4. The passage describes the verification of a PIN by comparing a PIN stored in a database with a transmitted PIN. But the description is only of a single PIN that is transmitted, from which the verification is performed. There is no teaching or suggestion that a pair of PINs are part of a payment service request.

The last passage cited by the Office Action is:

> FIG. 8 illustrates the operation of the service agent software for assigning a new PIN number where a customer desires a new PIN or has forgotten the PIN number. The service agent first inputs the customer name and any other identifying data that is available, along with the desired new PIN number (step A). The old PIN could also be required, except for a lost PIN. This information is then transmitted to the ETC processor computer (step B). The ETC processor computer compares the account information to determine whether there is sufficient information to claim that account (step C). If there is insufficient or non-matching information, an error message is returned (step D).
>
> Otherwise, the PIN number assigned to that account is updated (step E). The new PIN number is also transmitted to the PCAS issuer record database in the VisaNet system for updating as well (step F). Finally, an acknowledgement message is returned to the service agents software (step G).
>
> (Levine, Col. 7, ll. 39 – 55).

This passage is cited in the Final Office Action at p. 5, l. 6 and at p. 8, l. 4, and describes the updating of a PIN, such as might be performed "where a customer desires a new PIN or has

forgotten the PIN number." It does not teach or suggest that a pair of PINs be part of a payment service request.

It is apparent that the various passages cited from Levine merely describe such routine operations as updating a PIN or verifying a PIN. Such operations never involve a pair of PINs as part of a payment service request.

ii. IBM

Appellant acknowledges that IBM discloses the use of two PINs as the Final Office Action asserts (*e.g.* Final Office Action, pp. 2 and 3). But its disclosure of how those two PINs are used is different from what is claimed. Specifically, IBM teaches that the two PINs are available for use by user to perform different functions, with only a single one of the PINs ever being provided as part of a service request:

> The basic idea of this disclosure is the dual PIN access modes which provide two PINs for you credit, ATM or smart cards. Both PINs will allow the card owner to perform the function the card supposed to do. But the second PIN will provides additional functions than the first PIN. If someone is forced to withdraw money from the bank with one's ATM card by the criminal, one can simply punch in the second PIN of one's ATM card. This will perform additional functions, such as sending a silent robbery alarm to the police or the security guard in addition to allow one to withdraw cash successfully. In this case, the criminal even doesn't know that his or her crime has been reported.
> (IBM, p. 1)

As indicated in the cited portion, when a customer provides one of the PINs, certain functions may be accessed by the user, such as conventional functions accessible to customers possessing a card and knowing the PIN. When another of the PINs is provided, additional or different functions may be accessed by the user, such as secretly indicating that functions are being performed under duress. In each instance, though, only a single one of the PINs is provided to access functionality. IBM neither teaches nor suggests a service request that has a pair of PINs.

b. Claims 1 – 15

Independent Claim 1 is patentable over the cited art because the art fails to teach or suggest the claim limitation of "processing a payment service request having ... a pair of ATM network compatible PINs." As noted in the discussion of the prior art above, nothing in any of the cited references teaches the inclusion of a pair of PINs in a payment service request, the description in all of the references always being limited to the use of a single PIN in a service request. Indeed, both Levine and IBM teach away from use of such a pair of PINs by teaching exclusive use of a single PIN in service requests, a factor that has long been recognized as indicating that the combination is *not* obvious. Claims 2 – 15 are also patentable over the cited art by virtue of their dependence from a patentable claim.

c. Claims 40 – 54

Independent Claim 40 is patentable for substantially the same reasons. Specifically, the cited art does not teach or suggest "a processor for processing a payment service request having ... a pair of ATM network compatible PINs." Since the cited art is limited to disclosing the inclusion of only a single PIN in a service request, it does not teach or suggest the claim limitation. Dependent Claims 41 – 54 are also patentable over the cited art because they depend from a patentable claim.

d. Claims 61 – 69

Independent Claim 61 is patentable over the cited art because that art fails to disclose "providing an encoded data storage device to a user" that includes both "data representing a first ATM network compatible PIN [that is] a valid ATM PIN associated with said user's account at a financial institution" and "data representing a second ATM network compatible PIN [that is] an invalid ATM PIN not associated with said user's account at said financial institution." First, Levine fails to teach or suggest the inclusion of two PINs on an encoded storage device that is provided to a user. While Levine teaches certain updating functions, only a single PIN is even identified by the card described in that reference. Second,

while IBM teaches the use of two PINs, "[b]oth PINs will allow the card owner to perform the function the card [is] supposed to do" (IBM, p. 1). It clearly teaches away from the "data representing [the] second ... PIN [being] an invalid ATM PIN not associated with said user's account" (emphasis added), a factor that argues strongly that the proposed combination is *not* obvious. Because Claims 62 – 69 depend from Claim 61, they are similarly patentable over the cited art.

e. Claims 77 – 90

As previously noted, independent Claim 77 recites elements using means-plus-function language and approximately parallels independent system Claim 40. None of the cited art teaches or suggests a "means for generating a payment service request having ... a pair of ATM-network compatible PINs" for the reasons discussed above in connection with Claims 1 – 15 and 40 – 54. Namely, the cited art discloses the inclusion of only a single PIN in a service request. Claim 77 is accordingly patentable over the cited art, and Claims 78 – 90 are similarly patentable because of their dependence from Claim 77.

In its section captioned "Response to Arguments," the Final Office Action intimates that it is relying on certain claim limitations being inherent in the cited art. While Appellant agrees as a general matter that "[t]he express, implicit, and inherent disclosures of a prior art reference may be relied upon in the rejection of claims under 35 U.S.C. 102 or 103" (Final Office Action, p. 2, *citing* MPEP 2112), he disagrees that the relevant claim limitations are inherent in the cited art. The burden of establishing inherency is placed on the Examiner and is subject to a well-defined and rigorous standard: "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." MPEP 2112, *citing In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 – 51 (Fed. Cir. 1999). In this instance, no evidence has been provided that Levine or IBM necessarily require that a service request have a pair of ATM-network-compatible PINs. Indeed, the explicit descriptions in those

references make unambiguously clear that their service requests operate with a single PIN. The relevant limitations are thus manifestly not inherent in the cited art.

8. Conclusion

Appellant believes that the above discussion is fully responsive to all grounds of rejection set forth in the application. Please deduct the requisite fee of $500.00 pursuant to 37 C.F.R. §1.17(c) from Deposit Account 20-1430 and any additional fees that may be due in association with the filing of this Brief.

Respectfully submitted,

Patrick M. Boucher
Reg. No. 44,037

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
PMB:pmb
60730398 v1

CLAIMS APPENDIX

The claims involved in this appeal are as follows:

1. (Original) A method of providing a payment service including the steps of:

processing a payment service request having independent identification information and a pair of ATM network compatible PINs, including the steps of:

validating said independent identification information; and

generating an ATM network transaction message containing at least a selected one of said pair of ATM network compatible PINs based at least in part on said validating step; and

forwarding said ATM network transaction message to a financial institution over an ATM network for payment.

2. (Original) The method of claim 1 further including the step of:

providing a data storage device for interacting with a network access device; said data storage device having said pair of ATM network compatible PINs stored thereon;

wherein each one of said pair of ATM network compatible PINs is independently encrypted and different from one another.

3. (Original) The method of claim 2 further including the step of:

generating said payment service request including said pair of ATM network compatible PINs and independent identification information.

4. (Original) The method of claim 3 further including the step of authorizing payment to a payee.

5. (Original) The method of claim 3 wherein said payment service request further includes an amount.

6. (Original) The method of claim 4 wherein said payment service request further includes an amount.

7. (Original) The method of claim 1 wherein said independent identification information comprises an electronic personal identification number.

8. (Original) The method of claim 1 wherein said validating step includes:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

9. (Original) The method of claim 7 wherein said validating step includes:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

10. (Original) The method of claim 9 wherein based at least in part on said validating step said ATM network transaction message includes a valid ATM network compatible PIN.

11. (Original) The method of claim 9 wherein said ATM network transaction message includes an invalid ATM network compatible PIN.

12. (Original) The method of claim 1 wherein said payment service request further includes a payee.

13. (Original) The method of claim 1 further including inputting said independent identification information at a network access device.

14. (Original) The method of claim 7 further including inputting said independent identification information at a network access device.

15. (Original) The method of claim 7 wherein said electronic personal identification number comprises a number other than a user's ATM network compatible PIN.

16. – 39. (Canceled).

40. (Original) A system for providing a payment service including:

a processor for processing a payment service request having independent identification information and a pair of ATM network compatible PINs, said processor configured to:

validate said independent identification information;

generate an ATM network transaction message containing at least a selected one of said pair of ATM network compatible PINs based at least in part on said validation;

and forward said ATM network transaction message to a financial institution over an ATM network for payment.

41. (Original) The system of claim 40 further including:

a data storage device for interacting with a network access device; said data storage device having said pair of ATM network compatible PINs stored thereon; wherein each one of said pair of ATM network compatible PINs is independently encrypted and different from one another.

42. (Original) The system of claim 41 wherein said processor is further configured to generate said payment service request including said pair of ATM network compatible PINs and independent identification information.

43. (Original) The system of claim 42 wherein said financial institution authorizes payment to a payee.

44. (Original) The system of claim 43 wherein said payment service request further includes an amount.

45. (Original) The system of claim 44 wherein said payment service request further includes an amount.

46. (Original) The system of claim 40 wherein said independent identification information comprises an electronic personal identification number.

47. (Original) The system of claim 40 wherein said processor is further configured to validate said independent identification information by:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

48. (Original) The system of claim 46 wherein said processor is further configured to validate said independent identification information by:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

49. (Original) The system of claim 48 wherein based at least in part on said processor validation said ATM network transaction message includes a valid ATM network compatible PIN.

50. (Original) The system of claim 48 wherein based at least in part on said processor validation said ATM network transaction message includes an invalid ATM network compatible PIN.

51. (Original) The system of claim 40 wherein said payment service request further includes a payee.

52. (Original) The system of claim 40 further including an input device for inputting said independent identification information at a network access device.

53. (Original) The system of claim 46 further including an input device for inputting said independent identification information at a network access device.

54. (Original) The system of claim 46 wherein said electronic personal identification number comprises a number other than a user's ATM network compatible PIN.

55. – 60. (Canceled).

61. (Original) A method of a providing payment service comprising the steps of:

providing an encoded data storage device to a user; said encoded data storage device including:

data representing a first ATM network compatible PIN; wherein said first ATM PIN is a valid ATM PIN associated with said user's account at a financial institution;

data representing a second ATM network compatible PIN; wherein said second ATM PIN is an invalid ATM PIN not associated with said user's account at said financial institution;

providing independent identification information associated with said user's account at said financial institution;

validating said independent identification information;

generating a payment service request including a selected one of said first ATM PIN or said second ATM PIN based upon said validating step; and

forwarding said payment service request to said user's financial institution over an ATM network for further processing.

62. (Original) The method of claim 61 wherein encoded data storage device further includes a primary account number associated with said user's bank account stored thereon.

63. (Original) The method of claim 61 wherein said encoded data storage device further includes a bank identification number stored thereon.

64. (Original) The method of claim 61 wherein said generated payment service request is stored by a merchant for forwarding to a financial institution at a selected time.

65. (Original) The method of claim 61 wherein said forwarded payment service request is forwarded to said financial institution a plurality of times.

66. (Original) The method of claim 61 wherein said independent identification information comprises an electronic personal identification number.

67. (Original) The method of claim 61 wherein said payment service request further includes an amount.

68. (Original) The method of claim 61 wherein the step of forwarding said payment service request to said user's financial institution over an ATM network for further processing further includes authorizing payment to a payee.

69. (Original) The method of claim 61 wherein a merchant provides said independent identification information and data representing said first ATM network compatible PIN and said second ATM network compatible PIN received by a user to a processor for validating said independent identification information and generating said payment service request.

70. – 76. (Canceled).

77. (Original) A system for providing a payment service including:

first means for generating a payment service request having independent identification information and a pair of ATM network compatible PINs;

second means for validating said independent identification information;

third means for generating an ATM network transaction message containing at least a selected one of said pair of ATM network compatible PINs based at least in part on said validation; and

fourth means for forwarding said ATM network transaction message to a financial institution over an ATM network for payment.

78. (Original) The system of claim 77 further including:

fifth means for storing data and interacting with a network access device; said data storage means having said pair of ATM network compatible PINs stored thereon; wherein each one of said pair of ATM network compatible PINs is independently encrypted and different from one another.

79. (Original) The system of claim 78 wherein said financial institution authorizes payment to a payee.

80. (Original) The system of claim 79 wherein said payment service request further includes an amount.

81. (Original) The system of claim 80 wherein said payment service request further includes an amount.

82. (Original) The system of claim 77 wherein said independent identification information comprises an electronic personal identification number.

83. (Original) The system of claim 77 wherein said second means is further configured to validate said independent identification information by:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

84. (Original) The system of claim 83 wherein said second means is further configured to validate said independent identification information by:

providing an independent identification information offset;

providing a transaction identifier representing an account number; wherein said transaction identifier does not represent said user's account number;

combining said user identification information and said offset to validate said user; and

associating said user identification information and said offset with said transaction identifier to validate a user.

85. (Original) The system of claim 85 wherein based at least in part on said second means validation said ATM network transaction message includes a valid ATM network compatible PIN.

85. (Original) The system of claim 85 wherein based at least in part on said second means validation said ATM network transaction message includes an invalid ATM network compatible PIN.

87. (Original) The system of claim 77 wherein said payment service request further includes a payee.

88. (Original) The system of claim 77 further including an input means for inputting said independent identification information at a network access device.

89. (Original) The system of claim 83 further including an input means for inputting said independent identification information at a network access device.

90. (Original) The system of claim 83 wherein said electronic personal identification number comprises a number other than a user's ATM network compatible PIN.

EVIDENCE APPENDIX

Not included.

PATENT

RELATED PROCEEDINGS APPENDIX

A copy of the Board Decision in Appeal No. 2005-2484 on U.S. Pat. Appl. No. 09/394,143 is attached.